Kim D. Stephens, OSB #030635
Chase C. Alvord, OSB #070590
TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, WA 98101
Telephone: (206) 682-5600
Facsimile (206) 682-2992

James J. Pizzirusso *(pending pro hac vice)*
Swathi Bojedla *(pending pro hac vice)*
HAUSFELD LLP
1700 K Street, NW Suite 650
Washington, D.C. 20006
Telephone: (202) 540-7200
Facsimile: (202) 540-7201

Attorneys for Plaintiff and the Proposed Class

UNITED STATES DISTRICT COURT

DISTRICT OF OREGON

PORTLAND DIVISION

MARSHALL COLCORD, on his own behalf and on behalf of all others similarly situated, **PLAINTIFFS**, v. **PREMERA BLUE CROSS, a Washington nonprofit corporation**, **DEFENDANT**.	Case No. **COMPLAINT – CLASS ACTION FOR DAMAGES** Breach of Contract Action (28 U.S.C. § 1332) DEMAND FOR JURY TRIAL

Plaintiff Marshall Colcord ("Plaintiff"), on his own behalf and on behalf of all others similarly situated ("Class Members"), brings this class action against Premera Blue Cross ("Premera" or "Defendant") and complains and alleges the following upon personal knowledge as to his own experiences and based upon information and belief as to all other matters:

I. INTRODUCTION

1. Defendant Premera is one of the largest health insurers in the Northwest United States. Plaintiff brings this case as a result of Premera's failure to properly secure and protect its users' sensitive, personally-identifiable information.

2. On March 17, 2015, Premera publicly disclosed that its information technology systems had been accessed in May 2014 by unauthorized users, resulting in the exposure of the confidential information stored in those systems, including names, dates of birth, emails addresses, physical addresses, telephone numbers, Social Security Numbers, member identification numbers, bank account information, and medical insurance claim information, including clinical information, dating back to 2002.

3. Premera's data security in its information technology systems was far below industry standards. Its data centers lacked access controls and other protocols and procedures to prevent unauthorized physical and/or logical access to Premera's customers' private data.

4. The U.S. Office of Personnel Management ("OPM") informed Premera its network lacked access controls and its information technology system and network security were vulnerable. As the Seattle Times reported, "Three weeks before hackers infiltrated Premera Blue Cross, federal auditors warned the company that its network security procedures were inadequate."[1]

5. Plaintiff and the Class Members he seeks to represent have been damaged by Premera's conduct, in that they paid more than they would have had they known that Premera would fail to properly secure, as well as misuse, their personal information. Additionally, Plaintiff and the Class Members have been damaged because they purchased and used services of a quality different than they were promised and for which they contracted.

6. Plaintiff brings this action as a class action seeking all appropriate damages and

[1] Mike Baker, *Feds warned Premera about security flaws before breach*, Mar. 18, 2015, http://www.seattletimes.com/business/local-business/feds-warned-premera-about-security-flaws-before-breach/. (last visited Mar. 18, 2015).

remedies available to him and members of the class proposed herein.

II. PARTIES

7. Plaintiff Marshall Colcord is an individual and, at all relevant times, was a resident of Multnomah County, Oregon. Plaintiff is insured through Premera.

8. Defendant Premera Blue Cross is a Washington nonprofit corporation, headquartered in Mountlake Terrace, Washington. It is one of the largest health plans in the Northwest United States and conducts business throughout Washington, Oregon, and Alaska. Its customers are located throughout the United States.

III. JURISDICTION AND VENUE

9. This Court has original subject matter jurisdiction over this Class Action pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d)(2). Class Members and the Defendant are citizens of different states within the meaning of 28 U.S.C. § 1332(d)(2)(A).

10. On information and belief, the proposed Class far exceeds 100 persons. Premera has estimated eleven million people have been affected by its data breach. Pursuant to 28 U.S.C. § 1332(d)(6), the aggregate amount of the Class Members' claims substantially exceeds $5,000,000 and thus exceeds the requisite amount in controversy set forth in 28 U.S.C. § 1332(d)(2).

11. Venue is proper in this judicial district pursuant to 28 U.S.C. § 1391(a) and (b) on the grounds that all or a substantial portion of the acts giving rise to the violations occurred in this judicial district.

12. The claims of Plaintiffs and the Class Members asserted in this Class Action Complaint are brought solely under state law causes of action and are governed exclusively by Oregon law. The claims of Plaintiffs and the Class Members are individual claims and do not unite or enforce a single title or right to which Plaintiffs and the Class have a common and undivided interest.

IV. FACTUAL ALLEGATIONS

Premera Promised to Protect Its Customers' Confidential Information

13. Premera maintains a Notice of Privacy Practices[2] that states it is "committed to maintaining the confidentiality of your [its customers] medical and financial information…" It further states that Premera is "required by law to protect the privacy of your [its customers] personal information…"[3] Premera's Notice of Privacy Practices also lists how Premera may use and disclose its customers' information.

In April 2014, the United States Office of Personnel Management Warned Premera That Its Information Technology Systems Were Vulnerable to Attack Because of Inadequate Security Precautions

14. Like many health insurance providers, Premera stores its customers' personal information, including their names, addresses, phone numbers, social security numbers, and health information on networked computer servers at one or more data centers.

15. However, unlike some other insurance providers' data centers, Premera's data centers lacked certain access controls and other protocols and procedures to prevent unauthorized physical and/or logical access to Premera's customers' private data.

16. The missing access controls included, but were not necessarily limited to, multi-factor authentication and "piggybacking" prevention for physical access to Premera's data center.

17. Premera also failed to maintain adequate network security to prevent and/or monitor unauthorized access to its computer networks, including those on which private customer data was stored.

18. In April 2014, OPM provided Premera with draft findings from its audit of Premera, which, among other things, outlined missing access controls and network security vulnerabilities.

19. For instance, Premera failed to implement software patches, including critical patches, service packs, and hot fixes, in a timely manner and lacked a methodology for

[2] Premera Blue Cross Notice of Privacy Practices, https://www.premera.com/wa/visitor/privacy-policy/ (last visited Mar. 18, 2015).
[3] *Id.*

ensuring it did not use unsupported or otherwise out-of-date software. The Federal Information System Controls Audit Manual ("FISCAM") and National Institute of Standards and Technology's Special Publication ("NIST SP") both state that organizations like Premera should frequently scan and update their computer software to detect, correct, and prevent system flaws and vulnerabilities.

20. One or more of Premera's servers contained software applications that were no longer supported by the software's vendors and that had known security vulnerabilities. FISCAM specifically states that organizations such as Premera should have procedures that "ensure only current software releases are installed in information systems. Noncurrent software may be vulnerable to malicious code such as viruses and worms."

21. One or more of Premera's servers were insecurely configured in a manner that could allow hackers or other unauthorized users to gain access to sensitive and proprietary information. NIST SP 800-53 Revision 4 specifically states that organizations such as Premera must perform scans of their systems for vulnerabilities and then remediate legitimate vulnerabilities.

22. Premera further failed to develop, document, and maintain a current server operating system baseline configuration, as required by NIST SP 800-53 Revision 4, for one or more of its servers. Without such a baseline configuration, Premera could not effectively audit its server and database security settings. The lack of such a baseline configuration also increased the risk that Premera's systems would not meet various performance and security requirements.

Unauthorized Users Gained Access to Premera's Information Systems in May 2014

23. On or about May 5, 2014, unauthorized users gained access to Premera's information technology systems and the confidential information stored in those systems, including information from insurance applicants; members of other Blue Cross Blue Shield plans who sought treatment in Washington, Oregon, or Alaska; and current and former Premera customers, whom Premera calls "members." That information included names, dates of birth,

emails addresses, physical addresses, telephone numbers, Social Security Numbers, member identification numbers, bank account information, and medical insurance claim information, including clinical information, dating back to 2002.

24. Premera has publicly claimed that it did not discover that unauthorized users had gained access to its information technology systems and the information stored on them until January 29, 2015,[4] nearly eight months after the unauthorized access occurred.

25. Premera did not publicly disclose that unauthorized users had accessed its information technology systems until March 17, 2015.

26. Premera has established a website, www.premeraupdate.com, on which it admits that "Attackers gained unauthorized access to our IT systems and may have accessed the personal information of our members, employees and other people we do business with."[5]

27. Premera has publicly stated that confidential information from approximately 11 million of its current and former customers may have been compromised, including those in the state of Oregon.[6]

V. FACTS RELATING TO NAMED PLAINTIFF

28. Plaintiff's insurance coverage through Premera commenced prior to May 2014. Plaintiff is a current Premera customer and cardholder.

29. In applying for and maintaining insurance with Premera, Plaintiff entrusted Premera with his private, confidential information, including his name, date of birth, email addresses, physical address, telephone number, Social Security Number, and insurance claim information, including clinical information.

30. At the time Plaintiff became a customer of Premera, and at all times since, he had a reasonable expectation that Premera would protect his confidential information from

---

[4] Premera Blue Cross, http://www.premeraupdate.com (last visited Mar. 18, 2015).
[5] *Id.*
[6] Coral Garnick, *Premera hit by cyberattack; 6 million in state may be affected*, Mar. 17, 2015, http://www.seattletimes.com/business/technology/premera-hit-by-cyberattack-11m-customers-may-be-affected/ (last visited Mar. 27, 2015).

unauthorized disclosure.

31. As a result of Premera's misrepresentations and actions, Plaintiff and the Class Members have suffered injuries including, but not limited to, the following:

a. Theft of their personal and financial information;

b. Costs associated with the detection and prevention of identity theft;

c. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the data breach, and the stress, nuisance, and annoyance of dealing with all issues resulting from the Premera data breach;

d. The imminent and impending injury flowing from potential fraud and identity theft posed by their personal and financial information being placed in the hands of hackers;

e. Money paid to Premera for health insurance during the period of the Premera data breach, in that Plaintiff and the Class Members would not have obtained insurance from Premera had Premera disclosed that it lacked adequate systems and procedures to reasonably safeguard customers' personal and financial information and had Premera provided timely and accurate notice of the Premera data breach;

f. Overpayments paid to Premera for health insurance purchased during the Premera data breach in that a portion of the price for insurance paid by Plaintiff and the Class Members to Premera was for the costs of Premera providing reasonable and adequate safeguards and security measures to protect customers' and insureds' personal and financial data, which Premera failed to do, and as a result, Plaintiff and the Class Members did not receive what they paid for and were overcharged by Premera; and

g. Continued risk to their personal and financial information, which remains in the possession of Premera and which is subject to further breaches so long as Premera fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' data in its possession.

VI. CLASS ACTION ALLEGATIONS

32. Plaintiff brings this lawsuit as a class action on his own behalf and all other Premera insureds who are similarly situated as members of a proposed plaintiff class pursuant to CR 23(a) and (b)(3). This action satisfies the numerosity, commonality, typicality, adequacy, predominance, and superiority requirements of those provisions.

33. The Class that Plaintiff seeks to represent is defined as follows:

> All individuals and entities in Oregon whose personal information was compromised as a result of the Premera Blue Cross data breach that occurred sometime between May 2014 and January 2015.

34. Excluded from the Class and Subclass are (a) Premera, any entity in which Premera has a controlling interest, and its legal representatives, officers, directors, employees, assigns and successors; and (b) the judge to whom this case is assigned and any member of the judge's immediate family.

Numerosity of Class and Ascertainability of the Class

35. Plaintiff is a representative of all other persons and entities who entrusted their private information to Premera. The similarly situated consumers are readily identifiable through Premera's own business records, including but not limited to application and enrollment records.

36. The potential members of the class as defined are so numerous that joinder of all Class Members is impracticable. Although the precise number of such consumers is unknown, Plaintiff believes that there are millions of class members.

Typicality

37. The claims of Plaintiff are typical of the claims of the Class he seeks to represent. Plaintiff and Class Members entrusted their personal information to Premera.

38. The factual bases of Premera's misconduct are common to all Class Members and represent a common thread of misconduct resulting in injury to all members of the Class.

39. Plaintiff and all Class Members have suffered damages resulting from Premera's wrongful conduct.

Predominance of Common Questions of Fact and Law

40. Questions of law and fact common to the class that predominate over any questions affecting only individual members of the Class, including without limitation and as alleged herein, the following:

a. Whether Premera failed to protect its customers' personal information with industry-standard protocols and technology;

b. Whether Premera's practices are false, misleading, or reasonably likely to deceive;

c. Whether Premera failed to disclose material facts relating to the character and quality of its data security practices;

d. Whether Premera's conduct was reckless;

e. Whether Premera's conduct constitutes a breach of contract; and

f. Whether Premera's conduct was negligent.

41. Resolution of these questions, which are common to all Class Members, will generate common answers that are likely to drive the resolution of this action.

Adequacy of Representation

42. The Named Plaintiff, Marshall Colcord, will fairly and adequately represent and protect the interests of the Class Members. The interests of Plaintiff and Plaintiff's counsel are not in conflict with those of the Class Members. Plaintiff and Plaintiff's counsel will prosecute this action vigorously on behalf of the Class Members. Plaintiff's counsel are competent and experienced in litigating large class actions and other complex litigation matters, including data breach cases.

Superiority of Class Action

43. Absent class treatment, Plaintiff and Class Members will continue to suffer harm and damages as a result of Premera's unlawful and wrongful conduct.

44. A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Without a class action, individual Class Members would face burdensome litigation expenses, deterring them from bringing suit or adequately protecting their rights. Class Members would continue to incur harm without remedy absent a class action, while Premera would continue to reap the benefits of its misconduct. In addition, class litigation is superior because it will obviate the need for unduly duplicative litigation that might result in inconsistent judgments about the legality of Premera's practices.

FIRST CAUSE OF ACTION – BREACH OF CONTRACT

45. Plaintiff realleges and incorporates all previous paragraphs as though fully set forth herein.

46. Plaintiff and the Class Members relied upon Premera's representations regarding privacy and data security before purchasing services from Premera.

47. Plaintiff and the Class Members entered into a contract for the purchase of services from Premera that included representations by Premera that it took steps to secure customers' private information, including, but not limited to, compliance with federal and state statutes, rules, and regulations governing privacy of information and preventing access to personal information except by employees and business associates.

48. Premera represented that it was required by law to abide by the terms of its confidentiality policy.

49. Plaintiff and the Class Members performed all obligations under the contract, if any, requisite to Premera's performance.

50. Plaintiff and the Class Members paid for, but never received, the privacy protections to which they were entitled. Part of the price of the services they purchased included security and data protection.

51. Premera's conduct constitutes breach of its contract with Plaintiff and the other Class Members.

52. Plaintiff, on his own behalf and on behalf of all other Class Members, seeks an award of damages in an amount to be proven at trial.

SECOND CAUSE OF ACTION – NEGLIGENCE

53. Plaintiff realleges and incorporates all previous paragraphs as though fully set forth herein.

54. Premera owed a duty to Plaintiff and the Class Members to exercise reasonable care in obtaining, retaining, and safeguarding customers' personal financial information.

55. Premera owed a duty to Plaintiff and the Class Members to adequately protect its customers' personal and financial information.

56. Premera breached its duties by (1) unreasonably allowing an unauthorized third-party intrusion into its computer systems; (2) failing to reasonably protect against such an intrusion; (3) unreasonably allowing third parties to access the personal and private financial information of its customers; and (4) failing to appropriately monitor its systems to detect unauthorized access.

57. Premera knew or should have known of its duties regarding security of private customer information, as well as the attendant risks of retaining personal and financial data and the importance of providing adequate security.

58. As a direct and proximate result of Premera's careless and negligent conduct, Plaintiff and the Class Members have suffered damages in an amount to be proven at trial.

59. Plaintiff and the Class Members expect that financial losses will grow as additional fraudulent use of customer's private information is discovered.

THIRD CAUSE OF ACTION – ACTIONABLE MISREPRESENTATION

60. Plaintiff realleges and incorporates all previous paragraphs as though fully set forth herein.

61. Premera was required to comply with certain standards for collection and securing of personal private data. In order to comply with those standards, Premera was required to adequately protect stored data and financial information, to monitor access to that

data, and not to disclose that data beyond authorized boundaries.

62. Plaintiff and the Class Members reasonably relied on the reasonable expectation that Premera, a large health insurance company, would comply with standards governing the collection and securing of private personal data.

63. Premera represented that it did comply with its obligations related to the security of personal private data.

64. Premera knew or should have known that it was not in compliance with its obligations to secure customers' personal and financial data.

65. Premera failed to communicate material information to Plaintiff and the Class Members regarding its non-compliance with its obligations to secure customers' personal and financial data.

66. Premera's failure to inform Plaintiff and Class Members that it was not in compliance with its obligations was a material omission, which it should have disclosed to Plaintiff and the Class Members.

67. Premera's representation that it was in compliance with its obligations was a material misrepresentation.

68. Premera knew that its data was insecure and continued to misrepresent it was otherwise.

69. Had Premera informed Plaintiff and the Class Members of its non-compliance with its obligations to secure customer personal and financial data, Plaintiff and the Class Members would have been better able to protect themselves from the damages they have incurred and continue to incur.

70. As a direct and proximate result of Premera's negligent and improper conduct, Plaintiff and the Class Members have suffered damages.

FOURTH CAUSE OF ACTION – UNJUST ENRICHMENT

71. Plaintiff realleges and incorporates all previous paragraphs as though fully set

forth herein.

72. Plaintiff and the Class Members conferred a monetary benefit on Premera in the form of monthly premiums.

73. Premera was aware of the benefit, and used the premiums to pay for the administrative costs of data management and security.

74. It would be unjust to allow Premera to retain the premiums conferred by Plaintiff and the Class Members because Premera failed to implement the data management and security measures that are mandated by industry standards.

FIFTH CAUSE OF ACTION – FAILURE TO TIMELY DISCLOSE BREACH UNDER ORS § 646A.604

75. Plaintiff realleges and incorporates all previous paragraphs as though fully set forth herein.

76. Premera is a business that conducts business in the state of Oregon and that owns or licenses computerized data that includes personal information.

77. On or about May 5, 2014, unauthorized users gained access to Premera's information technology systems, breaching the security of the information technology system that stored personal information. Premera allowed an unauthorized acquisition of computerized data that compromised the security, confidentiality, or integrity of personal information maintained by Premera.

78. Premera knew or should have known that the breach occurred, but due to its own negligent monitoring of its information technology systems containing personal information, did not discover the breach until January 29, 2015.

79. Premera did not notify the persons whose data was breached of the data breach until March 17, 2015.

80. Premera's failure to disclose the breach of the security of the system storing personal information until more than ten months after the breach occurred, and more than six

weeks after the breach was purportedly discovered, constituted unreasonable delay and was not a disclosure immediately following discovery of such breach.

81. As a direct and proximate result of Premera's failure to provide reasonably prompt disclosure, Plaintiff and the Class have suffered damages.

WHEREFORE, Plaintiff, on his own behalf and on behalf of all Class Members, seeks the following relief against Premera:

1. An order certifying this action as a class action under Fed. R. Civ. P. 23, and defining the Class as requested herein;

2. Damages in an amount according to proof, including actual, compensatory, and consequential damages incurred by Plaintiff and Class Members;

3. Disgorgement of premiums by which Premera was unjustly enriched;

4. Pre- and post-judgment interest on monetary damages;

5. An award to Plaintiff and Class Members of reasonable attorneys' fees and costs, to be paid by Premera;

6. Leave to amend the Complaint to conform to evidence produced at trial; and,

7. An award of such other and further relief as this Court may deem appropriate.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands trial by jury to the extent authorized by law.

Dated: March 27, 2015

Respectfully submitted,

TOUSLEY BRAIN STEPHENS PLLC

By: *s/ Kim D. Stephens*
Kim D. Stephens, OSB #030635

By: *s/ Chase C. Alvord*
Chase C. Alvord, OSB #070590

1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
Telephone: (206) 682-5600
Facsimile: (206) 682-2992
Email: kstephens@tousley.com
calvord@tousley.com

James J. Pizzirusso *(pending pro hac vice)*
Swathi Bojedla *(pending pro hac vice)*
HAUSFELD LLP
1700 K Street, NW Suite 650
Washington, D.C. 20006
Telephone: (202) 540-7200
Facsimile: (202) 540-7201
Email: jpizzirusso@hausfeld.com
sbojedla@hausfeld.com

Attorneys for Plaintiff and the Proposed Class